COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES APPROPRIATIONS FOR FISCAL YEAR 2015

THURSDAY, MARCH 27, 2014

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:02 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Barbara A. Mikulski (chairwoman) presiding.

Present: Senators Mikulski, Shelby, Murkowski, Kirk, and Boozman.

FEDERAL BUREAU OF INVESTIGATION

STATEMENT OF HON. JAMES B. COMEY, JR., DIRECTOR

OPENING STATEMENT OF SENATOR BARBARA A. MIKULSKI

Senator MIKULSKI. Good morning, everybody. The Subcommittee on Commerce, Justice, Science will come to order. This is our first hearing on the fiscal year 2015 budget. We are starting with the esteemed and much valued Federal Bureau of Investigation. We will have a two-part hearing. This will be an open session, with all Senators free to participate and ask their questions. When this concludes, we will adjourn for a classified hearing on the Bureau's needs, particularly in the global war against terrorism and cyber security and some of those that are more sensitive in terms of the need for global protection and global cooperation.

We want to welcome Director Comey here for his very important appearance and we look forward to hearing his testimony in terms of the needs of the FBI. Last year we concluded I think with a vote on January 20 in which we were able to pass an omnibus bill for fiscal year 2014. Thanks to the work, bipartisan and bicameral, Senator Murray and Congressman Ryan were able to give us a budget and a top line cancelling the sequester, which had a draconian impact on both the function of core agencies like the FBI and on the morale.

We look forward this year to moving ahead in an expeditious way to move this so that we could avoid that kind of crisis in budgeting that has been characteristic of the Congress for more now than 5 years.

To get our work done, we will again listen to Director Comey on budget and priorities. It is his first time as the Director, but not

our first meeting. We appreciate his competence, his candor and his long history of service.

In welcoming you, Mr. Director, we want to thank the entire FBI for the way that they protect America. Whether it is fighting crime in organized crime, whether it's dealing with terrorists or predators, the FBI is on the job 24-7, 365 days a year, and we want them to know that they're appreciated, and we would like to show our appreciation to make sure they have the right resources and the right tools so that they can do the job that they were signed up to do. We believe that they are the unsung heroes.

This hearing will focus on the FBI's vital work. As chair, I've reviewed the FBI's budget, which comes in at $8.4 billion. In fiscal year 2014 we had an increase of $762 million above the sequester request. So it was $762 million, and it sounds like it was a big bump-up, but it was a bump-up to keep us running in place.

I'd like you to describe then about your need to retain talent, to recruit talent, and to train and educate the legendary training that goes on at Quantico. I understand that the 2015 request would keep the FBI moving while making sure our taxpayer dollars are spent wisely.

Now, we know that the sequester caused the FBI to cancel training, to ration gas to 200 miles a week. We valued a much-read and circulated document called "Voices From the Field." This is where we heard from the FBI agents themselves. Not only did they fear furlough for their families, but they feared the impact on the mission. Then we heard they didn't have gas for their cars. What kind of—we can't do this. So we're going to make sure we're looking to you and listening to you to do this, so we'll be looking at the 21st century threats.

We know that one of the major 21st century threats is in cyber space, whether it's the hackers, the cyber spies, or the cyber terrorists. We want to be clear in this hearing that cyber security is not the cyber surveillance that is the subject of much discussion at many levels in this Government and in others. We know that cyber security means protecting us from criminals out to steal credit card information, personal identities, companies' trade secrets, and even worse, whether it's to bring down the grid or bring down our financial services.

We know the FBI's in the front line in this area, and that the request is $392 million for the Next Generation Cyber Initiative, $9 million less than 2014. So we want to know, what is it you want to do, either at this hearing or the classified one, and is this the resources to do it?

One of the hallmarks of the FBI has really been working with local law enforcement. The joint task forces that have emerged receive kudos from around the Nation. Certainly in my own Baltimore metropolitan area, in the Washington metropolitan area, law enforcement speaks with such enthusiasm and such energy when they talk about these joint task forces, and that they can rely on the FBI, but keep law enforcement. We don't have a national police force in this country, but we have an American joint task force.

So we want to know how in your budget, what this means to State and local. We've been concerned that these two face significant cuts.

Finally, I'd like to mention the fact that you need a new headquarters. We know that the Hoover Building is dated and to the point of even being dysfunctional, that you're in 20 leased spaces. You know that two alpha delegations, Maryland and Virginia, are duking it out. We'll go through the competitive process, but my criteria, wearing my national hat, is that you need full consolidation. You don't need a micro-consolidation, because we want it to meet its functionality and security requirements for the next 50 years.

So we look forward to listening to you and listening to the needs of really what is it to make sure how we have a robustly funded FBI, a 21st century FBI, for 21st century threats.

I now turn to my vice chairman, who's been such an advocate in this area and has some key facilities in Alabama, Senator Shelby.

STATEMENT OF SENATOR RICHARD C. SHELBY

Senator SHELBY. Thank you.

Mr. Director, I want to welcome you to the committee. This is your first appearance before the subcommittee as FBI Director. I hope you will be coming to see us often.

We had a good working relationship with your predecessor, Director Mueller, and we look forward to a similar relationship with you and the Bureau. The mission of the FBI is broad and multifaceted. Its responsibilities include, among other things, investigating terrorist attacks and cyber threats, targeting health care fraud, leading the Federal Government's efforts to analyze improvised explosive devices, routing out gang activity. The list goes on and on. You have a broad mandate.

This broad mission requires the FBI to maintain focus on traditional criminal activities, while adapting to the new threats of this country. Terrorists and criminals are agile and sophisticated. The same is required of the Bureau. To remain effective, the Bureau must have the ability, I believe, to refocus and retool to address emerging threats. Without a plan to address such threats or a process for regularly reevaluating priorities, the FBI will find itself playing catch-up with the criminal elements it seeks to eliminate.

The Bureau's 2015 budget, which is the subject of today's hearing, outlines the FBI's strategic priorities. According to the documents provided, these priorities have not substantially been redefined since 2011. This is particularly troubling given the growing cyber threat that the chairwoman mentioned that our Nation is facing.

Recognizing the dynamic world in which we live and the tough fiscal climate that we face here, I want to be sure that the budget priorities of the Bureau truly reflect the threats that are facing this country. The ultimate goal of any prioritization effort should be an FBI that is efficient, effective, and, more importantly, nimble for the foreseeable future.

I'm committed to working with you and the chair to ensure that we're targeting limited resources in a manner that safeguards taxpayer dollars while preserving public safety.

Once again, we appreciate you taking this job as the head of the Bureau and we look forward to working with you.

Thank you, Madam Chair.

Senator MIKULSKI. I want to acknowledge that Senator Kirk is here. Senator, could you hold your statement until the Director finishes and we turn to questions, or do you need to leave?

Senator KIRK. I will hold my statement.

Senator MIKULSKI. Thank you very much.

Director Comey.

SUMMARY STATEMENT OF HON. JAMES B. COMEY, JR.

Mr. COMEY. Madam Chairwoman, Senator Shelby, Senator Kirk, members of the subcommittee: it's an honor to be here representing the great people of the FBI. This is my first appearance in what is a 10-year term that I'm very, very excited about because of those people. I have spent my first 6 months traveling around trying to meet my troops, and what I discovered is that the magic of the FBI is its talent. We don't have a lot of stuff; we have remarkable people.

What I found when I first took this job was that they were people who were very stressed by the impact that sequester was having on them, which Senator Mikulski, you mentioned. Everywhere around the country I heard from my folks about the difficulties they were encountering with vacancies, limitations on gas, the abolition of training, and Quantico being a ghost town.

Thanks to this committee and other members of the Senate and the House, that changed in late January when the budget was passed. I'm now in a position where I'm restarting Quantico. I'm also looking to hire a thousand people to start to fill the almost 2,500 vacancies that we have—hundreds of special agents and intelligence analysts, to restock that magic of the FBI that is our talent.

So, thank you so much for that on behalf of the men and women of the FBI. And we need those people because, as Senator Shelby said, the plate of threats that we face is remarkable.

I'll start with our top priority, Counterterrorism. The threat that I've encountered returning to Government after 8 years away is one that remains incredibly serious, but has changed. It has metastasized in ways that are striking. The primary tumor along the border of Afghanistan and Pakistan was dramatically reduced by the fight of our men and women in uniform and our Intelligence Community. But at the same time, that threat has metastasized into the lightly governed or ungoverned spaces in the world, especially in North Africa, around the Gulf, and around the Mediterranean. And also here at home with the growth of the people we call homegrown violent extremists. I don't like to call them "lone wolves" because that sounds dignified in a way that they don't deserve—folks who are able to access Al-Qaeda's hateful propaganda on the Internet and convince themselves, even without being directed, that they need to engage in some sort of jihad here at home and kill innocent Americans. So that metastasizing threat poses an enormous challenge to everybody in the Intelligence Community, but especially to the great people of the FBI.

Counterintelligence remains a top priority of the Bureau because nation-states around the world still want to steal our secrets and they are finding new and sophisticated ways to do this, especially

through cyber. So we remain on guard 24-7, as the chairwoman said, to protect that which is most important to our Nation.

Cyber, as the chair said, touches everything I do. The reason is fairly easy to understand: we as Americans, as a Nation and as a people, have connected our entire lives to the Internet. It's where our children play, it's where our money is, it's where our health care is, it's where our infrastructure is, our secrets. So it's where those who would do us harm come at us—for our children, for our money, for our private information, for our Nation's secrets, and for our vital infrastructure. It touches everything the FBI is responsible for, so we are doing everything in our power to make sure we are deployed, equipped, and trained to address that threat.

And of course, we're responsible for a host of criminal challenges, from public corruption to civil rights to white-collar crime, gangs, human trafficking, and protecting our children. And we're doing that in 56 field offices all around this country and in offices all around the world every day.

As, Madam Chairwoman, you said, we also have a responsibility to use the taxpayers' money to train and to assist State and local law enforcement. We have world-class facilities and world-class technical capabilities and we work hard to make them available to our brothers and sisters in law enforcement.

The last thing I'll say is my travels have convinced me that the FBI is international in ways that would have been difficult to see just 10 years ago. Nearly everything we do that matters has an international dimension to it. So I am extremely proud of our legal attaches deployed around the world, who build relationships and do service for not just the FBI, but all the American people.

PREPARED STATEMENT

So we're doing a lot of things and we do it through the people. As I said, the magic is the talent. I thank you so much for supporting those folks and for giving me the resources to make sure we have enough of those great folks.

My hope for 2015 is to be able to sustain the progress we have made since late January, restock the talent of the FBI, and march out to meet those many challenges. I look forward to working with you on that.

Thank you so much.

[The statement follows:]

PREPARED STATEMENT OF HON. JAMES B. COMEY, JR.

Good morning Chairwoman Mikulski, Vice Chairman Shelby, and members of the subcommittee. I look forward to discussing the FBI's fiscal year 2015 budget request, as well as FBI programs and priorities for the coming year. On behalf of the men and women of the FBI, let me begin by thanking you for your ongoing support of the Bureau.

Thanks to the support of this subcommittee, we now have a budget in place that that allows us to do more operationally, to hire and train new agents and intelligence analysts, and to backfill vacant positions in our field offices. We pledge to be the best possible stewards of the budget you have provided for us and to use it to maximum effect to carry out our mission.

Today's FBI is a threat-focused, intelligence-driven organization. Each employee of the FBI understands that to mitigate the key threats facing our Nation, we must constantly strive to be more efficient and more effective.

Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security,

our economy, and our communities. These diverse threats facing our Nation and our neighborhoods underscore the complexity and breadth of the FBI's mission.

We remain focused on defending the United States against terrorism, foreign intelligence, and cyber threats; upholding and enforcing the criminal laws of the United States; protecting civil rights and civil liberties; and providing leadership and criminal justice services to Federal, State, municipal, and international agencies and partners. Our continued ability to carry out this demanding mission reflects the support and oversight provided by this committee.

The FBI's fiscal year 2015 budget request totals $8.3 billion in direct budget authority, including 34,970 permanent positions (13,050 Special Agents, 3,048 Intelligence Analysts, and 18,872 professional staff). This request includes two program enhancements: 14 positions and $3.2 million for Mutual Legal Assistance Treaty reform, and $15 million for operations and maintenance for the Terrorist Explosive Device Analytical Center (TEDAC) facility in Huntsville, Alabama.

Let me summarize the FBI efforts that this funding supports.

NATIONAL SECURITY

The FBI is the lead domestic intelligence and law enforcement agency in the United States. Our complementary intelligence and law enforcement capabilities make up the key components of the Bureau's national security mission. They also illustrate the unique authorities and mission we have in the U.S. Intelligence Community. We collect intelligence to understand and identify the threats to the Nation. And when the time comes for action to prevent an attack, we disrupt threats using our law enforcement powers through our Joint Terrorism Task Forces (JTTFs).

Much of the FBI's success can be credited to the longstanding relationships we enjoy with our intelligence, law enforcement, public, and private sector partners. With thousands of private and public business alliances and more than 4,100 JTTF members, including more than 1,500 interagency personnel from more than 600 Federal, State, territorial, and tribal partner agencies, the FBI's partnerships are essential to achieving our mission and ensuring a coordinated approach toward national security threats.

Counterterrorism

As the lead agency responsible for countering terrorist threats to the United States and its interests overseas, the FBI integrates intelligence and operations to detect and disrupt terrorists and their organizations.

Counterterrorism remains our top priority. The Boston Marathon bombings in April 2013 remind us that the terrorist threat against the United States remains persistent. The threat from homegrown violent extremists is of particular concern. These individuals present unique challenges because they do not share a typical profile; their experiences and motives are often distinct and personal. They are also increasingly savvy and willing to act alone, which makes them more difficult to identify and to stop.

In the past 2 years, homegrown extremists have attempted to detonate improvised explosive devices or bombs at such high profile targets as the Federal Reserve Bank in New York, commercial establishments in downtown Chicago, the Pentagon, and the U.S. Capitol. Fortunately, these attempts and many others were thwarted. Yet the threat from such individuals remains.

The foreign terrorist threat is similarly complex and ever changing. Overseas, we are seeing more groups and individuals engaged in terrorism, a wider array of terrorist targets, greater cooperation among terrorist groups, and continued evolution and adaptation in tactics and communication.

Al-Qa'ida and its affiliates, especially al-Qa'ida in the Arabian Peninsula (AQAP), continue to represent a top terrorist threat to the Nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October 2010.

To better address this evolving threat, the FBI has established the Countering Violent Extremism (CVE) Office. This office leverages FBI resources and works with Federal counterparts to empower our local partners to prevent violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the United States to commit acts of violence. The CVE Office facilitates an understanding of the catalysts to violent extremism, as well as its behavioral components and radicalization factors, and identifies possible inhibitors to these phenomena. The FBI is leading efforts to conduct outreach and raise community awareness, while upholding civil rights and civil liberties.

Counterintelligence

We still confront traditional espionage—spies posing as diplomats or ordinary citizens. But espionage also has evolved. Spies today are often students, researchers, or businesspeople operating front companies. And they seek not only state secrets, but trade secrets, research and development, intellectual property, and insider information from the Federal Government, U.S. corporations, and American universities. Foreign intelligence services continue to grow more creative and more sophisticated in their methods to steal innovative technology, critical research and development data, and intellectual property, which erodes America's leading edge in business and poses a significant threat to national security.

We remain focused on the growing scope of the insider threat—that is, when trusted employees and contractors use their legitimate access to information to steal secrets for the benefit of another company or country. This threat has been exacerbated in recent years as businesses have become more global and increasingly exposed to foreign intelligence organizations.

To combat this threat, the FBI's Counterintelligence Division educates academic and business partners about how to protect themselves against economic espionage. We also work with the defense industry, academic institutions, and the general public to address the increased targeting of unclassified trade secrets across all American industries and sectors.

Together with our intelligence and law enforcement partners, we must continue to protect our trade secrets and our state secrets, and prevent the loss of sensitive American technology.

Weapons of Mass Destruction

As weapons of mass destruction (WMD) threats continue to evolve, the FBI uses its statutory authorities to lead all investigations concerning violations of WMD-related statutes, preparation, assessment, and responses to WMD threats and incidents within the United States. The FBI provides timely and relevant intelligence analyses of current and emerging WMD threats to inform decision makers, support investigations, and formulate effective countermeasures and tripwires to prevent attacks.

To ensure an effective national approach to preventing and responding to WMD threats, the FBI created the Weapons of Mass Destruction Directorate integrating the necessary counterterrorism, intelligence, counterintelligence, and scientific and technological components into one organizational structure. Using this integrated approach, the Directorate leads WMD policy development, planning, and response to ensure its efforts result in a comprehensive response capability that fuses investigative and technical information with intelligence to effectively resolve WMD threats.

To enable the prevention or disruption of WMD threats or attacks, FBI headquarters personnel, 56 field WMD coordinators, and two WMD assistant legal attachés oversee implementation of national and international initiatives and countermeasures. The FBI conducts outreach and liaison efforts with critical infrastructure partners, the private sector, academia, industry, and the scientific community to implement tripwires that prevent any actor—terrorist, criminal, insider threat, or lone offender—from successfully acquiring chemical, biological, radiological, or nuclear material or dissemination equipment. Through these efforts, the WMD Directorate supports the broader work of the U.S. Government as a leading partner and active contributor to policy decisions.

The Counterproliferation Center (CPC) combines the operational activities of the Counterintelligence Division, the subject matter expertise of the Weapons of Mass Destruction Directorate (WMDD), and the analytical capabilities of both components to identify and disrupt proliferation activities. Since its inception in July 2011, the CPC has overseen the arrest of approximately 65 individuals, including several considered by the U.S. Intelligence Community to be major proliferators. Along with these arrests, the CPC has increased its operational tempo to collect valuable intelligence on proliferation networks.

Intelligence

The FBI's efforts to advance its intelligence capabilities have focused on streamlining and optimizing the organization's intelligence components while simultaneously positioning the Bureau to carry out its responsibilities as the lead domestic intelligence agency.

One way the FBI is enhancing our partnerships and our ability to address threats is through the Domestic Director of National Intelligence (DNI) Representative Program. Through this program, FBI senior-level field executives in 12 geographic locations are serving as DNI representatives throughout the United States. The Domes-

tic DNI Representatives are working with Intelligence Community partners within their regions to understand the threat picture and develop a more coordinated and integrated Intelligence Community enterprise. A more unified and effective Intelligence Community will enhance the Nation's ability to share information with our law enforcement and private sector partners, and will prevent and minimize threats to our national security.

In addition, we expanded the fusion cell model, which further integrates our intelligence and operational elements through teams of analysts embedded with agents in the operational divisions. These fusion cells examine the national and international picture and provide intelligence on current and emerging threats across programs, making connections that are not always visible at the field level. Providing standard criteria, these cells inform the Threat Review and Prioritization (TRP) process and develop National Threat Priorities for the field. The fusion cells assess the FBI's ability to collect intelligence to identify gaps, inform operational strategies, and mitigate threats to drive FBI operations. As a result, the fusion cells and TRP provide the field with clear guidance and a consistent process to identify priority threats, while ensuring FBI Headquarters has an effective way to manage and evaluate the most significant threats facing the country.

This strategic, national-level perspective ensures the FBI is developing a complete picture of the threat environment and directing our resources at priority targets to stay ahead of our adversaries. This integration provides a cross-programmatic view of current threats and enables a nimble approach to identifying and addressing emerging threats.

Cyber

We face cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us. They may seek to strike our critical infrastructure and our economy. The threat is so dire that cyber security has topped the Director of National Intelligence list of global threats for the second consecutive year.

Given the scope of the cyber threat, agencies across the Federal Government are making cyber security a top priority. Within the FBI, we are targeting high-level intrusions—the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We want to predict and prevent attacks, rather than reacting after the fact.

FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques—such as sources and wires, surveillance, and forensics—to fight cyber crime. We are working side-by-side with our Federal, State, and local partners on Cyber Task Forces in each of our 56 field offices and through the National Cyber Investigative Joint Task Force (NCIJTF). Through our 24-hour cyber command center, CyWatch, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to Federal cyber centers, government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber intrusion.

We also work with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance. And we are training our State and local counterparts to triage local cyber matters, so that we can focus on national security issues.

Our legal attaché offices overseas work to coordinate cyber investigations and address jurisdictional hurdles and differences in the law from country to country. We are supporting partners at Interpol and The Hague as they work to establish international cyber crime centers. We continue to assess other locations to ensure that our cyber personnel are in the most appropriate locations across the globe.

We know that to be successful in the fight against cyber crime, we must continue to recruit, develop, and retain a highly skilled workforce. To that end, we have developed a number of creative staffing programs and collaborative private industry partnerships to ensure that over the long term we remain focused on our most vital resource—our people.

CRIMINAL

We face many criminal threats, from complex white-collar fraud in the financial, healthcare, and housing sectors to transnational and regional organized criminal enterprises to violent crime and public corruption. Criminal organizations—domestic and international—and individual criminal activity represent a significant threat to our security and safety in communities across the Nation.

Public Corruption

Public corruption is the FBI's top criminal priority. The threat—which involves the corruption of local, State, and federally elected, appointed, or contracted officials—strikes at the heart of government, eroding public confidence and undermining the strength of our democracy. It impacts how well U.S. borders are secured and neighborhoods are protected, how verdicts are handed down in court, and how well public infrastructure such as schools and roads are built. The FBI is uniquely situated to address this threat, with our ability to conduct undercover operations, perform electronic surveillance, and run complex cases. However, partnerships are critical and we work closely with Federal, State and local authorities in pursuing these cases. One key focus is border corruption. The Federal Government protects 7,000 miles of U.S. land border and 95,000 miles of shoreline. Every day, more than a million visitors enter the country through one of 327 official ports of entry along the Mexican and Canadian borders, as well as through seaports and international airports. Any corruption at the border enables a wide range of illegal activities, potentially placing the entire Nation at risk by letting drugs, guns, money, and weapons of mass destruction slip into the country, along with criminals, terrorists, and spies. Another focus concerns election crime. Although individual States have primary responsibility for conducting fair and impartial elections, the FBI becomes involved when paramount Federal interests are affected or electoral abuse occurs.

Financial Crimes

We have witnessed an increase in financial fraud in recent years, including mortgage fraud, healthcare fraud, and securities fraud.

The FBI and its partners continue to pinpoint the most egregious offenders of mortgage fraud. With the economy and housing market still recovering in many areas, we have seen an increase in schemes aimed both at distressed homeowners and at lenders. Our agents and analysts are using intelligence, surveillance, computer analysis, and undercover operations to identify emerging trends and to find the key players behind large-scale mortgage fraud. We also work closely with the Department of Housing and Urban Development, Postal Inspectors, the IRS, the FDIC, and the Secret Service, as well as with State and local law enforcement offices.

Healthcare spending currently makes up about 18 percent of our Nation's total economy. These large sums present an attractive target for criminals—so much so that we lose tens of billions of dollars each year to healthcare fraud. Healthcare fraud is not a victimless crime. Every person who pays for healthcare benefits, every business that pays higher insurance costs to cover their employees, every taxpayer who funds Medicare, is a victim. Schemes can cause actual patient harm, including subjecting patients to unnecessary treatment, providing sub-standard services and supplies, and by passing potentially life-threatening diseases due to the lack of proper precautions. As healthcare spending continues to rise, the FBI will use every tool we have to ensure our healthcare dollars are used to care for the sick—not to line the pockets of criminals.

Our investigations of corporate and securities fraud have also increased substantially in recent years. As financial crimes become more sophisticated, so must the FBI. The FBI continues to use techniques such as undercover operations and Title III intercepts to address these criminal threats. These techniques are widely known for their successful use against organized crime, and they remain a vital tool to gain concrete evidence against individuals conducting crimes of this nature on a national level.

Finally, the FBI recognizes the need for increased cooperation with our regulatory counterparts. Currently, we have embedded agents and analysts at the Securities and Exchange Commission and the Commodity Futures Trading Commission, which allows the FBI to work hand-in-hand with U.S. regulators to mitigate the corporate and securities fraud threat. Furthermore, these relationships enable the FBI to identify fraud trends more quickly, and to work with our operational and intelligence counterparts in the field to begin criminal investigations when deemed appropriate.

Gangs/Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Today's gangs are sophisticated and well organized; many use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. Gangs do not limit their illegal activities to single jurisdictions or communities. The FBI is able to work across such lines, which is vital to the fight against violent crime in big cities and small towns across the Nation. Every day, FBI Special Agents work

in partnership with State and local officers and deputies on joint task forces and individual investigations.

FBI joint task forces—Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails Task Forces—focus on identifying and targeting major groups operating as criminal enterprises. Much of the Bureau's criminal intelligence is derived from our State, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets and our sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

Transnational Organized Crime

More than a decade ago, the image of organized crime was of hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or States. But organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion-dollar schemes from start to finish. These criminal enterprises are flat, fluid networks with global reach. While still engaged in many of the "traditional" organized crime activities of loansharking, extortion, and murder, new criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, identify theft, trafficking of women and children, and other illegal activities. Preventing and combating transnational organized crime demands a concentrated effort by the FBI and Federal, State, local, and international partners. The Bureau continues to share intelligence about criminal groups with our partners, and to combine resources and expertise to gain a full understanding of each group.

Crimes Against Children

The FBI remains vigilant in its efforts to eradicate predators from our communities and to keep our children safe. Ready response teams are stationed across the country to quickly respond to abductions. Investigators bring to this issue the full array of forensic tools such as DNA, trace evidence, impression evidence, and digital forensics. Through improved communications, law enforcement also has the ability to quickly share information with partners throughout the world, and our outreach programs play an integral role in prevention.

The FBI also has several programs in place to educate both parents and children about the dangers posed by predators and to recover missing and endangered children should they be taken. Through our Child Abduction Rapid Deployment teams, Innocence Lost National Initiative, Innocent Images National Initiative, Office of Victim Assistance, and numerous community outreach programs, the FBI and its partners are working to keep our children safe from harm.

The FBI established the Child Sex Tourism Initiative to employ proactive strategies to identify U.S. citizens who travel overseas to engage in illicit sexual conduct with children. These strategies also include a multi-disciplinary approach through partnerships with foreign law enforcement and non-governmental organizations to provide child victims with available support services. Similarly, the FBI's Innocence Lost National Initiative serves as the model for the partnership between Federal, State and local law enforcement in addressing child prostitution. Since its inception, more than 3,100 children have been located and recovered. The investigations and subsequent 1,450 convictions have resulted in lengthy sentences, including twelve life terms.

Indian Country

The FBI continues to maintain primary Federal law enforcement authority to investigate felony crimes on more than 200 Indian reservations nationwide. More than 100 Special Agents from 20 different field offices investigate these cases. In addition, the FBI has 14 Safe Trails Task Forces that investigate violent crime, drug offenses, and gangs in Indian Country and we continue to address the emerging threat from fraud and other white-collar crimes committed against tribal gaming facilities.

Sexual assault and child sexual assault are two of the FBI's investigative priorities in Indian Country. Statistics indicate that American Indians and Alaska Natives suffer violent crime at greater rates than other Americans. Approximately 75 percent of all FBI Indian Country investigations concern homicide, crimes against children, or felony assaults.

The FBI continues to work with tribes through the Tribal Law and Order Act of 2010 to help tribal governments better address the unique public safety challenges and disproportionately high rates of violence and victimization in many tribal communities. The act encourages the hiring of additional law enforcement officers for

Native American lands, enhances tribal authority to prosecute and punish criminals, and provides the Bureau of Indian Affairs and tribal police officers with greater access to law enforcement databases.

SCIENCE & TECHNOLOGY

Laboratory Services

The FBI Laboratory ("the Lab") is one of the largest and most comprehensive forensic laboratories in the world. Operating out of a state-of-the-art facility in Quantico, Virginia, laboratory personnel travel the world on assignment, using science and technology to protect the Nation and support law enforcement, intelligence, military, and forensic science partners. The Lab's many services include providing expert testimony, mapping crime scenes and conducting forensic exams of physical and hazardous evidence. Lab personnel possess expertise in many areas of forensics supporting law enforcement and intelligence purposes, including explosives, trace evidence, documents, chemistry, cryptography, DNA, facial reconstruction, fingerprints, firearms, and WMD.

One example of the Lab's key services and programs is the Combined DNA Index System (CODIS), which blends forensic science and computer technology into a highly effective tool for linking crimes. It enables Federal, State, and local forensic labs to exchange and compare DNA profiles electronically, thereby connecting violent crimes and known offenders. Using the National DNA Index System of CODIS, the National Missing Persons DNA Database helps identify missing and unidentified individuals.

TEDAC is another example. TEDAC was formally established in 2004 to serve as the single interagency organization to receive, fully analyze, and exploit all priority terrorist Improvised Explosive Devices (IEDs). TEDAC coordinates the efforts of the entire government, including law enforcement, intelligence, and military entities, to gather and share intelligence about IEDs. These efforts help disarm and disrupt IEDs, link them to their makers, and prevent future attacks. Although originally focused on devices from Iraq and Afghanistan, TEDAC now receives and analyzes devices from all over the world.

Additionally, FBI Evidence Response Teams (ERTs) are active in all 56 field offices and include more than 1,200 members. The FBI supports and enables evidence collection capabilities of field ERTs and law enforcement partners by providing forensic training, resources, and expertise. The FBI also has forward-deployed evidence response capabilities to respond to terrorist attacks and criminal incidents involving hazardous materials (chemical, biological, nuclear, and radiological) in concert with local officials and FBI WMD experts.

Operational Technology

Terrorists and criminals are increasingly adept at exploiting cutting-edge technologies to carry out or to mask their crimes. To counter current and emerging threats, the FBI actively deploys a wide range of technology-based tools, capabilities, and training that enable and enhance intelligence, national security, and law enforcement operations. In addition to developing state-of-the-art tools and techniques, the FBI also focuses on recruiting and hiring individuals who possess specialized skills and experience. These dedicated employees serve as technically trained agents, engineers, computer scientists, digital forensic examiners, electronics technicians, and other specialists. Collectively, these specialists enable lawful electronic surveillance, provide secure communications, decipher encrypted messages, reverse engineer malware, forensically examine digital evidence such as images and audio recordings, and much more.

By way of example, the National Domestic Communications Assistance Center (NDCAC) is designed to leverage and share the law enforcement community's collective technical knowledge, solutions, and resources to address the challenges posed by advancing communications services and technologies. The NDCAC also works on behalf of Federal, State, local, and tribal law enforcement agencies to strengthen law enforcement's relationships with the communications industry.

The FBI has also established 16 Regional Computer Forensic Laboratories (RCFLs) across the Nation. RCFLs serve as one-stop, full-service forensics laboratories and training centers. All RCFL personnel in each of the 16 facilities across the country must earn FBI certification as digital forensics examiners and follow standardized evidence handling and operating procedures. RCFLs are staffed by Federal, State, and local law enforcement personnel who examine digital evidence in support of all types of investigations—cases involving everything from child pornography and terrorism to violent crime and economic espionage.

Criminal Justice Information Services

The FBI Criminal Justice Information Services (CJIS) Division, located in Clarksburg, West Virginia, provides Federal, State, and local enforcement and other authorized users with timely access to criminal justice information through a number of programs, including the National Crime Information Center, the Uniform Crime Reporting program, and the National Instant Criminal Background Checks System.

In addition, CJIS manages the Integrated Automated Fingerprint Identification System (IAFIS), which provides timely and accurate identification services by identifying individuals through name, date-of-birth, fingerprint image comparisons, or other descriptors, and provides criminal history records on individuals for law enforcement and civil purposes. IAFIS is designed to process criminal fingerprint submissions in 2 hours or less and civil submissions in 24 hours or less. In fiscal year 2013, approximately 62.7 million fingerprint background checks were processed. The Next Generation Identification program advances the FBI's biometric identification and investigation services, providing new biometric functionality such as facial recognition, improved latent searches, and immediate responses related to the Repository for Individuals of Special Concern, a fingerprint index of wanted persons, sexual offender registry subjects, known or appropriately suspected terrorists, and other persons of special interest.

CJIS also manages the Law Enforcement National Data Exchange (N–DEx), a criminal justice information sharing network that allows law enforcement agencies to share law enforcement records from more than 4,500 agencies with nearly 140,000 criminal justice users. The N–DEx network contains more than 225 million searchable records (incident reports, arrest reports, booking data, etc.). It is projected that by the end of fiscal year 2014, N–DEx information sharing will be available to law enforcement agencies representing almost 60 percent of the U.S. population.

CRITICAL INCIDENT RESPONSE GROUP

The Critical Incident Response Group (CIRG) is a "one stop shop" for responding rapidly to crisis situations worldwide. Its professionals are on call around the clock, ready to support FBI operations and Federal, State, local, and international law enforcement partners in managing critical incidents and major investigations.

The National Center for the Analysis of Violent Crime (NCAVC) provides operational support to FBI agents and law enforcement personnel on complex and time-sensitive cases.

The Behavioral Threat Assessment Center (BTAC) assesses the potential threat of violence posed by persons of concern and as reflected in threatening communications. Issues traditionally addressed by the BTAC include school and workplace attacks, threats against Members of Congress and public figures, and threatening communications.

The Violent Criminal Apprehension Program (ViCAP) is the national repository for violent crime cases—specifically those involving homicides, sexual assaults, missing persons, and unidentified human remains—helping to draw links between seemingly unconnected crimes. In 2008, the FBI launched the ViCAP Web National Crime Database, which is available to law enforcement agencies through the secure Law Enforcement Online (LEO) website. Investigators can search ViCAP Web for nationwide cases similar to theirs and communicate with other U.S. law enforcement agencies to coordinate investigations based on these linkages. More than 5,000 Federal, State, and local law enforcement agencies have contributed to the 85,000-case ViCAP national violent crime database.

Active Shooter Training

In the aftermath of the tragedy at Sandy Hook elementary school, the President announced the Now Is the Time initiative focused on protecting children and communities by reducing gun violence. A critical component of this initiative focuses on schools, institutions of higher education, and houses of worship. The FBI was assigned to lead law enforcement training to ensure coordination among agencies. To that end, we have trained more than 9,600 senior State, local, tribal, and campus law enforcement executives at conferences hosted by FBI field offices, and trained more than 6,300 first responders through tabletop exercises designed around facts similar to recent school shootings. To date, the FBI has provided our Advanced Law Enforcement Rapid Response Training course, an active shooter training program, to more than 1,400 officers from 613 agencies.

Tactical Operations & Crisis Response

CIRG has a range of tactical resources and programs that support and provide oversight to the FBI and its partners. For example, each FBI field office has a

SWAT team that is equipped with a wide array of specialized weaponry and is trained to engage in hazardous operations such as barricaded subjects, high-risk arrest/search warrants, patrolling through adverse terrain, and—in some field offices—maritime interdictions. These teams include crisis negotiators who routinely respond to prison sieges, hostage takings, and kidnappings nationwide and provide assistance to State and local police negotiators. CIRG also manages the FBI Hostage Rescue Team—the U.S. Government's non-military, full-time counterterrorist tactical team—which provides enhanced manpower, training, and resources to confront the most complex threats.

The Hazardous Devices School at Redstone Arsenal in Huntsville, Alabama, is the Nation's only facility for training and certifying public safety bomb technicians to render safe hazardous devices. Managed by the FBI, the school has trained more than 20,000 State and local first responders since it opened in 1971. A natural extension of this school can be found in the FBI's own 249 Special Agent bomb technicians, who provide training to local and State bomb squads and serve as the workforce for the FBI's explosives-related operations worldwide.

VICTIM ASSISTANCE

Through the Office for Victim Assistance (OVA), the FBI ensures that victims of crimes investigated by the FBI are afforded the opportunity to receive the services and notifications required by Federal law and the Attorney General Guidelines on Victim and Witness Assistance. Among its many services, OVA provides on-scene help to crime victims, assesses and triages their needs, and helps victims identify and secure counseling, housing, medical attention, and legal and immigration assistance. When other resources are not available, OVA administers special Victims of Crime Act funds to meet victims' emergency needs, including reunification travel, crime scene cleanup, replacement clothing, and shipment of victims' remains.

Special services are provided to child victims. The Child Pornography Victim Assistance Program coordinates support and notification services for child victims of pornography and their guardians. The Forensic Child Interviewing Program ensures that investigative interviews of child victims and witnesses of Federal crimes are tailored to the child's stage of development and minimize any additional trauma. Additionally, a detailed protocol was recently developed for providing support to families of abducted children and assisting with post-recovery reunification and follow-up services. OVA is partnering with the Criminal Investigative Division's Violent Crimes Against Children Section and other agencies and organizations to improve the response to and services for minor victims of sex trafficking.

The Terrorism and Special Jurisdiction Program provides emergency assistance to injured victims and families of American victims killed in terrorist attacks and serves as a permanent point of contact for terrorism victims. Victim Assistance Rapid Deployment Teams provide immediate, on-scene assistance to victims of domestic terrorism and mass violence, often at the request of local law enforcement agencies. These highly trained and experienced teams have responded to numerous mass casualty crimes since 2006, most recently to tragedies at Sandy Hook Elementary School, the Washington Navy Yard, and at the Boston Marathon.

INFORMATION TECHNOLOGY

The FBI's Information and Technology Branch (ITB) provides enterprise-wide IT products and services to more than 36,000 FBI employees, contractors, and task force members, including managing more than 114,000 workstations and 46 mission-critical systems.

The target of the ITB's current modernization efforts is to create the future FBI Information Environment. Technology provides a distinct advantage, allowing FBI users access to their critical data when, where, and how they need it. The FBI Information Environment will support development of new mission and business functionality within a defined and controlled IT framework. These modernization efforts will move the FBI toward an agile, responsive, and efficient services-based operating model, emphasizing reuse of enterprise services both to increase cost savings and to enhance the reliability of IT infrastructure and applications.

INTERNATIONAL OFFICES

One of the fundamental challenges of the 21st Century is stopping overseas threats from compromising the security of the United States. For this reason, the FBI maintains more than 80 offices overseas that cover more than 200 countries and territories. Though our successes have been many, the increase in crimes with an overseas nexus shows we must do more.

The FBI continues to look for opportunities to open offices worldwide in the Middle East, Africa, Eurasia, the Americas, and Asia to target emerging terrorist, cyber, and criminal threats. Staff have strong cross-programmatic skills and work side-by-side with sister agencies, host governments, and corporate partners to take on threats. By targeting terrorists and criminals on their home turf—before their plots take shape—the FBI can stop those who wish to harm the United States before they have the capability to do so.

TRAINING

In fiscal year 2014, the FBI plans to graduate approximately seven new groups of trainees by the end of the fiscal year—more than 300 Special Agents. We also hope to fill six classes of new intelligence analysts.

The National Academy provides law enforcement executives and investigators from State and local law enforcement agencies worldwide with advanced leadership training. The National Academy has continued to trained more executives, adding to its total of more than 47,000 graduates to date.

The FBI provides leadership, intelligence, and law enforcement assistance to its international training partners through a variety of programs designed to establish and strengthen cooperation and liaison between the FBI and its overseas counterparts. Courses offered include organized crime cases, anti-gang strategies, terrorist crime scene investigations, and street survival techniques. The FBI also administers the International Law Enforcement Academy (ILEA) in Budapest, Hungary, and supports other academies in Bangkok, Thailand; Gaborone, Botswana; and San Salvador, El Salvador; as well as the Regional Training Center in Lima, Peru. The curriculums of these academies are based on the FBI National Academy model. To date, more than 11,100 students have received ILEA training.

Other key training programs include Leadership in Counterterrorism, which has trained more than 400 upper-level counterterrorism executives from State or national police agencies and chiefs or deputy chiefs of local agencies to date; the Domestic Security Executive Academy, which has trained more than 340 Federal executives and Fortune 1,000 corporate security executives; the Law Enforcement Executive Development Seminar (LEEDS), a two-week program designed for chief executive officers of the Nation's mid-sized law enforcement agencies; and the National Executive Institute (NEI), a two-week executive training program that provides strategic leadership education and partnership opportunities for executives from the highest levels of the FBI and the largest U.S. and international law enforcement agencies.

LEADERSHIP DEVELOPMENT

We created the Leadership Development Program (LDP) to help prepare FBI employees to lead before taking formal leadership positions, by providing relevant tools, courses, and developmental experiences needed for success. These efforts are fostering a Bureau-wide cultural shift toward promoting long-term individual development to better operate in quickly developing transitions and crises.

Since 2009, LDP has built a variety of integrated programs, including onboarding for both new employees and specific positions such as executives and senior managers, in-depth courses for both current and new supervisors and program managers, and a developmental program to prepare aspiring leaders before they are promoted. LDP's various programs were created by employees, for employees, and are designed to build upon one another over the course of an employee's career. They were originally benchmarked against successful models from our military, law enforcement, and intelligence partners, as well as private companies; as LDP has grown, other government agencies now reach out to benchmark against the FBI.

OFFSETS

The FBI's fiscal year 2015 budget request includes an offset of $168 million to pay for increases in existing costs, including pay raises, Federal Employees Retirement System contributions, State Department charges, and General Services Administration (GSA) rent, among others. The offset will be achieved through a combination of program efficiencies and administrative savings. In addition, the fiscal year 2015 request includes a $12 million offset to the Secure Work Environment (SWE) program. In fiscal year 2015, the SWE program will continue to maintain existing facilities while providing an increase in capabilities at high priority locations.

CONCLUSION

Responding to this complex and ever-changing threat environment is not new to the FBI. The resources this subcommittee provides each year are critical for the FBI's ability to address existing and emerging national security and criminal threats.

Chairwoman Mikulski, Vice Chairman Shelby, and members of the subcommittee, I would like to close by thanking you for this opportunity to discuss the FBI's priorities. Chairwoman Mikulski, we are grateful for the leadership that you and this subcommittee have provided to the FBI. We would not be in the position we are today without your support. Your investments in our workforce, our technology, and our infrastructure make a difference every day at FBI offices in the United States and around the world, and we thank you for that support.

I look forward to answering any questions you may have.

Senator MIKULSKI. Well, that was very compelling testimony, Director. I think it was organized in the way our priorities are in terms of our national security threats, our criminal threats, support to our partners, particularly in our country, and those that are around the world.

BUDGET

But the FBI is, in terms of its $8 billion—and I think it's a bargain for what we get for $8 billion, when you think of the magnitude, of the number of agents, the analysts, the support staff, 60 places around the world, 56 field offices here.

But your request really goes to people. It's not a big plane, it's not a big aircraft carrier. What we were able to do in fiscal year 2014 on a bipartisan basis I think allowed you to bring in 1,000 new critical positions; is that right?

Mr. COMEY. Yes, which I'm trying to fill by October 1.

Senator MIKULSKI. Now, what in terms of—what is it that we need to help you keep that momentum going? The talent is not a spigot you can turn on. Unlike—and we're not knocking our friends in defense, but you know you can delay the purchase of an aircraft carrier, you can buy one less fighter plane, save a half a billion dollars. But here talent, both the trainers that you need, again at Quantico, and then the ability to recruit—people, they don't want to be in a spigot job; they want to be in a real job, you know, where the spigot's on.

Tell us what we need to do in our line items to really sustain the momentum and provide the adequacy in particularly key areas?

Mr. COMEY. Thank you, Senator Mikulski. As you said, the FBI is people. I have no battleships, no satellites. I have great men and women. What I need is to be able to hire the people that I'm trying to hire by October 1st and then continue to hire, because we're down almost 2,500 positions. So I need to be able to hire the new folks next fiscal year and pay and support those that we bring on this year. So just to continue the progress is what I need.

Senator MIKULSKI. The purpose of this hearing is not fiscal year 2016, but then the biggest threat to your momentum would be not a stringent budget in fiscal year 2016, but a sequester that just goes across the board; is that correct?

Mr. COMEY. Yes, that would be sort of back to the future for us. If that were to happen, we'd again be in the position where we'd be rationing gas and not filling vacancies, and we'd be back to what we experienced the last 2 years.

STATE AND LOCAL LAW ENFORCEMENT

Senator MIKULSKI. Now, let's go to State and local law enforcement in my time. These partnerships are key. We don't have a national police force. America doesn't want it. But we have an FBI that provides national resources and deals with Federal crime.

You, meaning the Federal level, rely on local law enforcement to be eyes, ears, boots on the ground. It's the local police commissioner and the local police officer that often sees something and says something that makes a difference, whether it's fighting crime or dealing with the terrorist threat.

I note a cut in the State and local law enforcement area. What do you anticipate in order, again, to sustain and maintain the relationships and the effort at the local level, like fighting gangs that I know Senator Kirk is so devoted to, a great concern of mine in the Baltimore area, the whole issue of child predators and the trafficking in children. So could you share with us then what you need in that area?

Mr. COMEY. Certainly, Senator. There's nothing we do—not nothing we do at all, but certainly nothing we do that matters, that we don't do in partnership with State and local law enforcement. The days of the lone fed are long gone. We work together to make sure we're gaining maximum leverage from each other, whether that's protecting kids, protecting neighborhoods, or protecting the Nation from terrorists.

A bedrock of our counterterrorism response is our Joint Terrorism Task Forces. We have over 100. They are 50 percent State, local, and other Federal law enforcement agencies. So those partnerships are vital. Part of the glue that holds those partnerships together is our ability to offer training and technical assistance to our brothers and sisters at the State and local level. We had to shut all that down before the budget was passed at the end of January. So now we are again offering that training and assistance, and I'd like to be able to continue that.

Senator MIKULSKI. There are other questions that I have, but I'm going to yield to Senator Shelby.

Senator SHELBY. Thank you, Madam Chair. I'll try to be brief, but I have a number of questions, Madam Chair.

CYBER SECURITY

Director Comey, you've acknowledged the growing cyber security threat that was mentioned by the chair, facing our Nation and the challenges that are inherent in facilitating private industry reporting of attacks. It's been told to us that private industry often believes that their reports fall on deaf ears because they receive no feedback or little feedback or follow-up information about the status of some of the reports. This perception could be a serious impediment to the kind of information-sharing that you envision. I think it's important.

My question is what steps are you taking or will you take to foster relationships with private industry and in turn increase the number of private industry participants in the Bureau's reporting system, which I think is essential here? And would you also speak directly to the concerns regarding the industry reporting process

and the fact that the information exchange is perceived as a one-way street? You know, it's got to be both because you have to rely on a lot of that.

Mr. COMEY. Thank you, Senator. Great question and a really important topic. One of the many great things about our amazing country is that our Internet is almost entirely in private hands. That's the way it should be. That's the engine of entrepreneurship and creativity in this country. One of the challenges that poses is that without the ability to share information effectively between the government and private enterprise, the law enforcers are left patrolling a street that, if you imagine, almost has 30-foot high solid walls on either side. I can declare that the street is safe, but I'm not really protecting the neighborhood because it's on the other side of the wall.

We have to find a way to share information in both directions, consistent with protecting the great liberties that underlie this country. So we at the FBI, and the Federal Government as a whole, have to get better at sharing actionable information with the private sector; not just telling them there's a problem in your system, but telling them, here's what it is, here's what it means, here's what you can do about it. And they need to do the same. They have a lot of smart people in private industry. When they see something, they've got to be able to share it with us.

So there are two things need to be done. We have to get better, and we're developing a whole host of ways to be more effective at our information-sharing. And we have to offer them clear rules of the road, so when they're looking to share information with us they understand how it will be used and how it might affect their shareholders, if it exposes them to lawsuits, and all the other things that come in this great country. So that bipartisan clarity needs to be offered.

Senator SHELBY. You're going to work on that, aren't you?

Mr. COMEY. We're working like crazy on that.

Senator SHELBY. That's good.

HAZARDOUS DEVICES SCHOOL

The Hazardous Devices School. The FBI's Hazardous Devices School trains and certifies public safety bomb technicians. You know this well.

Mr. COMEY. Yes, sir.

Senator SHELBY. In addition to providing basic training for bomb technicians, the Hazardous Devices School of the Bureau is also responsible for providing training in electronic countermeasures and advanced training in priority threat scenarios. State and local technicians are the first line of defense in responding to bomb threats, working with the Bureau. Ensuring that they're aware of the latest trends and are properly trained I think is very important and this school does a lot of this.

Could you talk just for a few minutes about the training capacity of your Hazardous Devices School today, specifically the number of students that it can accommodate, the number of classes offered annually, and the need that exists in terms of recertifying, as we evolve, the bomb technicians? And is there an unmet training need

in the community, and if so how can we address it, because we've got 300 million people and we do have some threats.

Mr. COMEY. Yes. Thank you, Senator. We have many.

One of the hidden gems of this country is the Hazardous Devices School, where, as you said, Senator, we train all bomb techs in the United States. So it's an effort that's a joint Federal effort that includes the Department of Defense, which is a key partner in the Hazardous Devices School. So it is a vital basic building block for people who want to become special agent bomb techs or want to become bomb techs in police departments.

What we need to do to make sure we're taking advantage of that gem is be able to offer advanced training certifications for people who have gone out and become bomb techs to come back to get refresher training and to get advanced training on the latest devices and threats. So we've done a good job at offering the basic training. What we need to find a way to do is to re-source that additional training and sophisticated refresher training for those bomb techs.

Senator SHELBY. You're going to have to get ahead of the terrorists in many ways, are you not?

Mr. COMEY. Yes.

Senator SHELBY. Because if you lag behind technically speaking, we're in a real threat area.

Mr. COMEY. Yes, sir. There are smart, evil people laying awake at night trying to find ways to defeat us and to find the next thing that we haven't caught up with. We need to be just as smart and just as wide awake.

TERRORIST EXPLOSIVE DEVICE ANALYTICAL CENTER

Senator SHELBY. The Terrorist Explosive Device Analytical Center, as we call it, TEDAC, is the single inter-agency organization to receive, fully analyze, and exploit all terrorist improvised explosive devices, or IEDs. Much of the TEDAC's work has come from Iraq and Afghanistan. But as U.S. forces withdraw from Afghanistan, TEDAC's focus will shift. I believe that the IED threat that we face at home or could face in the future makes the work of TEDAC probably more important than ever.

What's the FBI's vision for a postwar TEDAC and will the skills and capabilities shift with the threat, and if so what will it look like? Because you've got to be nimble here. Although we've been fortunate and the Bureau's done a great job and other law enforcement people, we can't be so smug or secure to think that people can't build those improvised explosive devices here, because they can. What are your thoughts in this?

Mr. COMEY. That's exactly right, Senator. TEDAC is a lifesaver. It has saved lives in Afghanistan and in Iraq. It saves lives all around the world. And I agree with you completely, the drawdown in Iraq and Afghanistan will not signal a drawdown in terrorist efforts to kill us with these explosive devices. In fact, what's happened is a lot of the terrorists have learned techniques in the war zones that they're now looking to spread around the world. So we have to stay on top of our game there. We need to continue to make sure we're drawing on the military for their advice and guidance. But TEDAC will save lives for the indefinite future because the threat is indefinite.

Senator SHELBY. Madam Chair, I have a couple of more questions that I'd like to submit for the record for the Director, because I know we have another closed hearing after this.

Senator MIKULSKI. Without objection, so ordered.

I want to turn now to Senator Boozman, but before I do I want to acknowledge that Senator Kirk was here. He has a longstanding interest and advocacy in this area.

We're doing 60 hearings in 6 weeks to move our deadlines. So Senators are stretched. But we want to also acknowledge that if Senator Kirk has any questions we'll submit them to the record. We also know his longstanding interest in fighting gangs, as we noted, and I'm sure he'll have questions in this area.

Senator Boozman.

Senator BOOZMAN. Thank you, Madam Chair, very much.

Thanks for being here. We appreciate you and appreciate the great job that the FBI does and the dedication that's represented there.

AGRICULTURE ESPIONAGE

Recently in Arkansas we had a situation where some people were arrested for espionage in the farm sector. I'd like for you to talk about that a little bit. I think there's a lot of surprise that we saw that in Arkansas, again in the farm sector. Something I think is really important, it's kind of like—I'm an optometrist by training, an eye doctor, and so it's much better to prevent things than it is to let them happen. Can you talk a little bit about some of the things that you are doing, some of the things you'd like to do that aren't getting done, to really make our companies, make us as a Congress, aware that these things are going on, how we can help you in that regard?

ESPIONAGE

Mr. COMEY. Yes, thank you, Senator. There's no doubt that foreign nation-states, especially China, want to steal our ideas. The ideas of America are not just in Internet companies. They're often in the creative work that agriculture companies are doing to develop disease-resistant seeds or crops that will produce greater yields with less water, things that will help people.

The source of that entrepreneurship and that energy are the great people here in the United States working in labs and working in companies. There are countries around the world that, rather than do that work, would like to steal it from us, which would sap that energy and that entrepreneurship and kill that spirit that's at the center of this country.

So it's something we focus on constantly. It's the reason we have counterintelligence at the top of our list, because there are people in cases that we've brought who are looking to steal seed technology, every bit as much as people want to steal intellectual property on the Internet. So what we're doing is trying to make sure we're aggressive in those cases, so that when we catch folks doing that, they understand there's a cost to it. We're going to lock people up for that. It's not a freebie to take America's seed technology. And we're trying to put in place tripwires so that companies, whether it's agricultural companies or whether it's a software com-

pany, understand when they see something that doesn't seem right to them, they've got to call us, because bad people are looking to steal things that matter to you enormously.

Those tripwires are very valuable and contributed in the case that you were referring to and other cases that we've brought that relate to agricultural theft.

Senator BOOZMAN. Very good.

CYBER SECURITY

In a related area, cyber security, certainly you are doing a lot in that regard, I think hopefully in educating and again in getting after folks that are doing that. The private sector is doing a pretty good job of that, and the private sector has a tendency to perhaps be a little bit more innovative or move a little quicker with things. Can you talk about some of the public-private partnerships that you're pursuing in that regard, or are you pursuing public-private partnerships?

Mr. COMEY. Yes, we are, Senator, for the reasons you said. I spent the last 8 years working at two world-class companies in two different industries and there's no doubt that private industry is spending the money to get the talent on board to think in a good way about those challenges. So they've got a lot of brainpower.

We have to be smart by connecting ourselves to that brainpower. I've got a lot of smart people. I don't have all the smart people in the world. A whole lot of them are in private enterprise. So as I said in response to Senator Shelby, we have to get better at connecting ourselves.

Therefore a bunch of different ways in which we're trying to do that. We have an effort called Infraguard, where we're trying to join together in partnership all around the country with private industry. We have something called DSAC, the Domestic Security Alliance Council, to accomplish the same mission. But whatever it's name, we need to make sure we're connected to them.

One of the obstacles is we live in a litigious society—I was the general counsel of two companies and I know as the general counsel you worry: if I cooperate with the government, is someone going to sue me, claim that I violated some obligation to protect information? It's one of the reasons I think it's so important that we, through legislation, offer those clear rules of the road to those general counsels so they can tell their tech geeks, you can go ahead and share this and here's what the rules are.

LEGAL ATTACHÉ OFFICES

Senator BOOZMAN. You mentioned in your testimony about opportunities to establish offices worldwide, in the Middle East, Africa. Can you talk about some of the barriers that you're running into in that regard or some of the obstacles perhaps that you face in trying to get that done?

Mr. COMEY. Well, in our Legal Attaché program—we call them "LEGATs"—we have 64, I think that is the number, around the world. I have visited now ten of them and discovered that they are, as I said, not just a representative of the FBI, but of the entire United States, a tremendous force multiplier for us.

So the obstacle is I simply need to make sure that I identify more good people and have the resources to develop those offices at embassies around the world. So I'm going to be looking to do more of that early in my tenure. It's simply a question of identifying the talent and having the resources to do it.

Senator BOOZMAN. Thank you, Madam Chair.

Senator MIKULSKI. Thank you, Senator.

The question of the international assistance I think is really something the committee needs to pay attention to. I believe there are 60 LEGAT offices around the world. Am I correct?

Mr. COMEY. I think the number is 64.

Senator MIKULSKI. Some are micro, but some are robust in countries where we need to be robust or have been invited?

Mr. COMEY. Yes, that's exactly right.

Senator MIKULSKI. And they're not secret. They're known. In other words, the private sector—first of all, the host country knows, etcetera.

Mr. COMEY. That's correct.

Senator MIKULSKI. They're usually cooperating locally and working regionally; am I correct?

Mr. COMEY. That's correct, Senator.

Senator MIKULSKI. You want to add 14—the President's budget and I believe yours is 14 positions, for a modest $3.2 million; is that correct?

Mr. COMEY. That's correct. That's what I meant by the resources to spread that great thing a little bit farther out.

Senator MIKULSKI. Yes. And it would mean a lot to some of these countries for us to have a presence?

Mr. COMEY. Oh, yes. I got a call this morning with a foreign counterpart who asked me about that. They find them incredibly valuable as a gateway that swings both ways. It gets our country information, but also helps them get assistance, especially training for their law enforcement.

Senator MIKULSKI. And a presence, that the FBI is not the KGB.

Mr. COMEY. We are not.

Senator MIKULSKI. That's what I hear a lot.

Mr. COMEY. Nice to show people that.

Senator MIKULSKI. Yes.

Senator Murkowski.

Senator MURKOWSKI. Thank you, Madam Chairman.

Good morning, Director. I appreciate your leadership here. A couple years ago when your predecessor, Director Mueller, appeared before our subcommittee—this was in 2012—Senator Hutchison, who served on the committee as well, she and I asked him about the possible FBI misconduct in the investigation and the prosecution of Senator Ted Stevens. I'm assuming or I'm hopeful that in preparation for today's hearing your staff might have told you that it was a whistleblower complaint of an FBI agent named Chad Joy that first brought the misconduct to light.

EMPLOYER MISCONDUCT RELATING TO STEVENS INVESTIGATION

I haven't heard anything about the FBI's probe into Agent Joy's allegations since 2012. So the question that I have for you this morning: The Director at that meeting told the committee that the

FBI's investigation of employee misconduct is still pending relating to the Stevens investigation. That was 2 years ago. We're here in 2014. So the question is whether or not the FBI's investigation has been concluded and, if so, what was the outcome of that investigation, and if there has been any corrective action taken if you could inform me?

SENATOR STEVENS INVESTIGATION

Mr. COMEY. Yes, Senator. Thank you for the question and for the opportunity to update you. I did learn about this in the last week and get briefed in detail. The Office of Professional Responsibility, OPR, inside FBI did investigate in response and identified an agent who had engaged in improper conduct, and the agent was severely disciplined. The discipline has been imposed. On top of that, we pushed out refresher training to the entire workforce, especially about our discovery obligations and how we expect them to conduct themselves during those investigations.

So both broad remedial work was done and individual discipline was imposed for the agent involved.

Senator MURKOWSKI. Was there a report that was prepared, and if so would you be able to provide the subcommittee with a copy of that?

Mr. COMEY. I don't know—I'm sure something was written up because we always have written support for discipline imposed. I'll check and get back to you on it.

[The information follows:]

OPR REPORT ON TED STEVENS CASE AGENT

Sensitive employee personnel information is contained in Office of Professional Responsibility reports. As such, the FBI can provide a briefing on these documents in an appropriate setting.

Senator MURKOWSKI. I'd appreciate that.

I had also asked about whether or not the agent who had brought this issue to the forefront, Agent Joy, had received any recognition from the FBI for really stepping up there. Director Mueller indicated at that time he didn't know whether or not there had been anything that had been done to recognize Agent Joy.

In fact what happened was that Agent Joy left the Bureau. He believes that his career was undermined by the whistleblowing. Again, as you are looking to this issue, if you might look into this specific situation regarding Agent Joy and really whether or not the Bureau did right by him, because I think we all pay attention to what goes on with whistleblower situations, but if there is a perspective or a view within the agency that not only are whistleblowers not rewarded, but in fact there are consequences, negative consequences at the end, that's something that I think we need to certainly be aware of.

Mr. COMEY. Thank you for raising that. I don't know, but I'll find out.

[The information follows:]

AGENT JOY WHISTLEBLOWING

The FBI can provide a briefing on this sensitive personnel matter in an appropriate setting.

Senator MURKOWSKI. I appreciate that.

Mr. COMEY. Because I share your belief that whistleblowers are essential to a healthy institution. And I have a practice now where I call individual agents and support people around the country to thank them, for not famous acts, but for good pieces of work. So I'm going to follow up and find out where this fellow is, because maybe it's worth a phone call from me.

Senator MURKOWSKI. I appreciate that.

HUMAN TRAFFICKING IN NATIVE COMMUNITIES

One final question then for you, and this relates to human trafficking in our Native communities, not a subject that any of us want to talk about particularly, but I think that this is an area that is grossly underreported. Research that documents the extent of a problem is often done in the universities and think tanks. My alma mater out in Oregon, Willamette University Law School, released a report on the extent of human trafficking in Oregon. In Alaska, it's the Salvation Army that has made the note that Natives are one of the populations most vulnerable to human trafficking. Traffickers apparently will sell Alaska Native women and girls believing that their ethnicity is more appealing to buyers. It sickens you to even be discussing it.

The FBI budget document speaks to the Bureau's role in human trafficking, but it doesn't specifically address the commitment of resources to human trafficking that involves Native women, American Indians or Alaska Native women. We all know that this problem is continuing to grow. So I'd ask what the Bureau is doing today to address the problem, what more you could be doing in these areas, and in terms of your statistical capabilities to what extent is the Bureau able to track to victimization of American Indians, Alaska Native women who are trafficked, and is there more that we can do to focus on this demographic?

Mr. COMEY. Thank you for the question. The answer is I don't know, but it's something that I need to get smarter about, because I learned a lot in the 6, 7 months I've been on the job about human trafficking and I've been shocked by it, just as you are, and about crime in Native American communities. But I have not thought well about this specific human trafficking issue in Native American communities, but I will.

This question of research is also very interesting to me. I don't know whether we do a good enough job at the national level to think well about the problem. Chairman Wolf in the House has suggested that maybe we ought to add that capability to the National Gang Intelligence Center, so that we have people who wake up every morning thinking about it holistically, which is also something I'm going to look at.

But I will get smarter and get back to you.

[The information follows:]

HUMAN TRAFFICKING OF NATIVE AMERICANS

The FBI is actively engaged in efforts to identify and combat human trafficking involving tribal communities. The FBI has strengthened its work through ongoing collaboration with U.S. Attorney's Offices and other Federal, State, local, and tribal partners. Through these partnerships, the FBI provides training, conducts investiga-

tions, and supports trafficking victims in tribal areas, including, in South Dakota and the Bakken oil-producing region of North Dakota and Montana.

In January 2014, the FBI Office for Victim Assistance collaborated with the FBI Civil Rights Unit and Violent Crimes Against Children Section, as well as the Department of Health and Human Services, to conduct Webinar trainings for FBI personnel to commemorate National Slavery and Human Trafficking Prevention Month. Training topics included: coordinating large scale operations that focus on domestic minor sex trafficking; human trafficking in Indian Country and the Bakken region of North Dakota and Montana; identifying resources and services available to adult and foreign minor victims of human trafficking; and, understanding and identifying labor trafficking.

Senator MURKOWSKI. I appreciate that. We have resources clearly in Alaska that have been looking very specific to the issues as it relates to Alaska Native women, and I know your folks on the ground up north are very capable in this area. But if we can have a broader understanding as to the issue in this country as it relates to our indigenous people, particularly our women and girls, I think it would be a very important focus.

Thank you, Madam Chairman.

Senator MIKULSKI. The vice chairman has an additional question. I just would like to amplify what Senator Murkowski has said. Both she and then Senator Cantwell, who chaired our Committee on Indian Affairs that's Pacific Northwest-focused, have spent a lot of time really on what is happening to Native Americans in this country and particularly the women and the children. They're not only a great resource to you, but a great way for you, to point you to these resources where a lot of work has been done, but not a lot of action has happened.

Does that summarize it, Senator?

Senator MURKOWSKI. Yes.

Senator MIKULSKI. So look to us here and we can help you get smart about it, and then let's get a real action plan.

Senator Shelby.

Senator SHELBY. Thank you, Madam Chair.

CHILD EXPLOITATION AND CHILD PORNOGRAPHY

I want to follow up on this area, Mr. Director. I have visited Eastern Europe and the Ukraine and other areas where a lot of the human trafficking of young women that have been abused, to say the least, as you well know, into forced prostitution of different kinds, child pornography, everything, just small children. That is a big, big business, especially the child pornography. It's international in scope. It's obviously—it's hard to stamp out.

But in America, a lot of Americans are buying movies of this. It's sickening. But on the Banking Committee I remember Senator Sarbanes—I was chairman on the committee and he was ranking, and then he was chairman and I was ranking. We worked together on this a lot, dealing with the payment system, because the key is the credit card system, how do you pay for it?

The FBI and the Justice Department have been very good. It's very complex, very hard to discern everything. But it's one of the worst things that you could imagine, and you have. And if you have children or grandchildren or both, you think, my gosh. But the trafficking, the human trafficking of young women and young children and the exploitation of it is something that the Bureau has been

very good and the Justice Department. But it's such a massive thing to get our hands around.

Do you want to address that at all, and the FBI's interest here?

Mr. COMEY. It is a massive problem, as big as the Internet. The explosion of the Internet has brought with it an explosion in child exploitation and child pornography. It's an enormous machine that at the back end people are viewing child pornography, at the front end children are being fed into the engine. It's one of the reasons that it drives me a bit crazy when I hear people say: Oh, they were just looking at child pornography. Your just looking at child pornography, first of all, is sick in and of itself and raises serious concerns about whether you're abusing children in your own life.

Senator SHELBY. But it pays for it.

Mr. COMEY. Yes. But it's their desire to see fresh images that powers the engine at the front and leads to this voracious consumption of child pornography. So there's no such thing in my view as just looking at child pornography. It's a serious crime. It has to be taken seriously. It's something that, as Senator Mikulski knows—who is one of the great supporters of our "Innocent Images" program—it's something we are passionate about. We have to send a message both to those who would profit from the business, those who would view and become the consumers that drives this engine, and those who would touch the children and destroy them to produce those images. So we have to hit the whole train.

Senator SHELBY. Have you had real cooperation from, say, the people of the Ukraine and Russia and some of these other countries where a lot of this trafficking and filming and everything takes place?

Mr. COMEY. The answer is yes, because, despite what political differences we may have, all humans are revolted by the abuse of children, exploitation of children. So that's an area in which we can find common ground even with the folks in Russia.

Senator SHELBY. Thank you, Madam Chairwoman.

ADDITIONAL COMMITTEE QUESTIONS

Senator MIKULSKI. There are many more questions to be asked, but we're now going to move to our classified hearing. So this subcommittee will temporarily recess and reconvene in closed session at the secure facility in the Capitol Visitors Center, where we can consider those matters that require more classified conversation, particularly in the global war against terrorism, espionage, and these other vile, vile, and repugnant international crimes against children.

[The following questions were not asked at the hearing, but were submitted to the agency for response subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR PATRICK J. LEAHY

SHOOTING OF IBRAGIM TODASHEV

Question. What measures have you taken to ensure the American people that FBI shooting incidents, including the one in Florida last May, are investigated fairly and independently?

Answer. In 1982, then Director William Webster approved the establishment of the Shooting Incident Review Group (SIRG) which is comprised of the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) representatives to review and assess all shooting incidents involving FBI personnel. The SIRG pro-

vides the Director and FBI Headquarter Executive Management evaluative analyses, observations, and recommendations concerning operational, training, and other relevant issues, including the need for referral to the DOJ, Office of Inspector General (OIG), or the FBI's Internal Investigations Section for further administrative or disciplinary review, if deemed necessary. In 1995, the DOJ Office of Investigative Agency Policies adopted "Resolution 13," which further formalized the process by which DOJ investigative agencies conduct post shooting incident reviews. Central to "Resolution 13" was the requirement that the intentional and unintentional discharge of a firearm by a DOJ employee be expeditiously reported, documented, investigated, and reviewed.

In accordance with the establishment of the SIRG and "Resolution 13," the FBI utilizes a Shooting Incident Review Team (SIRT) to conduct an administrative inquiry of every Agent Involved Shooting (AIS) for the purpose of assessing and documenting the use of force incident, and to provide the DOJ Civil Rights Division sufficient information to make a prosecutorial determination. Each SIRT prepares a comprehensive report for the SIRG. Each SIRG meeting is attended by a representative of the DOJ OIG. The SIRG independently reviews FBI shooting incidents to determine whether the use of deadly force was reasonable, and in accord with the DOJ Deadly Force Policy and the law. The SIRT process is designed to inform affected field offices, and other FBI personnel, of findings or lessons learned from an operational, administrative, tactical, and training perspective.

The FBI routinely conducts AIS reviews in coordination with State and local authorities. FBI SIRTs jointly conduct post-shooting interviews and coordinate reporting to ensure both State/local and DOJ prosecutorial offices have information necessary to make an independent prosecutorial decision. DOJ and State/local prosecutors have independent, concurrent jurisdiction regarding Federal and State charges and coordinate with each other as appropriate.

FORENSICS REFORM

Question. Would you agree that there must be national leadership in the area of forensic science, and that the Department of Justice, working with the FBI and other elements of the executive branch, can play a central role in the development of this important part of our criminal justice system?

Answer. National leadership in the area of forensic science is of utmost importance. For over three quarters of a century, the Department of Justice and the FBI have served in such a leadership role, both nationally and internationally, for the forensic sciences.

Question. Will you commit to working with me on the forensics reform bill that I introduced today?

Answer. The FBI, in conjunction with other DOJ components takes the issue of improving forensics seriously and the Bureau would be glad to work with the Senator to provide feedback or technical assistance sought on legislation.

QUESTIONS SUBMITTED BY SENATOR JEFF MERKLEY

WHITE-COLLAR CRIME

Question. Could you please provide, in both real and proportional to the rest of the Department of Justice's (DOJ's) resources, what percentage of DOJ and the Federal Bureau of Investigation (FBI) resources have been dedicated to white-collar crime in general and mortgage fraud specifically over the past 20 years with a particular focus on times when high amounts of white-collar crime needed to be pursued, such as the economic fallout of the savings and loan crisis and the popping of the dot come bubble?

Answer. As an intelligence-driven, law enforcement and national security organization, the FBI has responsibility to address a variety of threats to include Terrorism, Counterintelligence, Cyber and a multitude of Criminal threats to include Public Corruption, Civil Rights, Organized Crime, Complex Financial Crime, and Violent Crime. Each year, the FBI utilizes intelligence to determine the appropriate ranking of those threats. Within the priority area of Complex Financial Crime, the FBI addresses the threats of Securities and Commodities Fraud, Corporate Fraud and Mortgage Fraud, among others.

Prior to the mortgage fraud crisis that emerged several years ago, the FBI did not track mortgage fraud separately, outside of its White-Collar Crime program, and thus cannot provide trends from the past 20 years. The chart below provides data since 2008.

WHITE-COLLAR CRIME

Type	2008	2009	2010	2011	2012	2013	2014
Department of Justice							
Mortgage Fraud	$ 69,546,000	$111,508,000	$151,984,000	$114,475,000	$141,308,000	$121,731,000	$129,338,000
Other White-Collar Crime	435,120,000	478,570,000	436,598,000	532,399,000	528,001,000	569,322,000	586,553,000
Total	504,666,000	590,078,000	588,582,000	646,874,000	669,309,000	691,053,000	715,891,000
Federal Bureau of Investigation							
Mortgage Fraud	32,203,000	66,763,000	94,287,000	70,131,000	69,048,000	53,564,000	59,497,000
Other White-Collar Crime	57,806,000	64,745,000	81,031,000	139,781,000	140,468,000	145,756,000	161,716,000
Total	90,009,000	131,508,000	175,318,000	209,912,000	209,516,000	199,320,000	221,213,000

Question. Please provide estimates in the differences in the resource costs required for the pursuit of individuals versus that of companies. Additionally, could you please provide estimates of resources required to prepare a case to be taken to court versus establishing non-prosecution and deferred prosecution agreements with companies?

Answer. Investigations into complex financial crimes commonly require the FBI to consider both individual and entity level criminal culpability. The investigations into individuals and entities have significant overlap as the individuals interviewed, documents analyzed, and investigative methods typically serve the dual purpose of uncovering the underlying facts, which may support charging individuals, entities, or both. Therefore, the FBI is unable to quantify the differences in resources required for the pursuit of an individual versus an entity. When investigating individuals, due to certain fact patterns, it is often appropriate to incorporate an investigation into the entity as well. An entity can also serve as a cooperator in investigations and the ultimate resolution reached with an entity can be significantly influenced by its level of cooperation, among other factors.

With regard to the differences in resources dedicated to investigations going to court versus those that end in non-prosecution agreements (NPAs) or deferred prosecution agreements (DPAs), the FBI's investigative strategy is one that rests on the assumption that all criminal investigations will be taken to trial. Doing so ensures a comprehensive investigation has been conducted and that the FBI is positioned to withstand the scrutiny of a trial by jury, if necessary. Conducting an investigation in this manner enables the FBI to more persuasively articulate the nature of the offenses and the evidence of those offenses by the targeted individuals, thereby increasing the likelihood of individual pleas or corporate resolutions without the need for a trial. For that reason, there is no significant difference in the cost for the FBI to investigate cases that proceed to trial and cases resolved without a trial.

CRIMINAL REFERRALS FROM FINANCIAL REGULATORY AGENCIES

Question. Please provide numbers for how many criminal referrals the FBI and DOJ has received from financial regulatory agencies year by year since 1990, broken down by referring agency. Has the number of criminal referrals from financial regulatory agencies changed over the past decade? Has there been a significant decline? If so, how does the FBI account for such a decline? What could the FBI do to train and encourage regulatory agencies to refer criminal activity for FBI investigation? Does the FBI have adequate resources to take on such activity?

Answer. The FBI does receive referrals from Federal regulatory agencies, but the number of referrals is not tracked; therefore, the FBI cannot assess trends in referrals. The FBI does work closely with other law enforcement and regulatory agencies to address complex financial crime. Understanding the current threat picture is essential to appropriately address the complex financial crime threat. FBI headquarters is actively engaged with private sector and other governmental agencies to understand the nationwide complex financial crime threat. This collaboration enables the development of a holistic view of the threat and identification of nationwide and local trends.

On a local level, the FBI is committed to working with local, State and Federal partners to investigate, prosecute, and collect and disseminate intelligence related to complex financial crimes. The FBI currently operates 21 Financial Crimes Task Forces throughout the United States. These task forces include at least 11 Federal agencies outside the Department, as well as partners within the Department, and over 30 local or State law enforcement and regulatory agencies. In total, the FBI

is dedicating nearly 900 agents and more than $200 million to combat corporate, mortgage, and securities fraud and other economic crimes.

The FBI recognizes the importance and value in continuing to build and maintain strong working relationships with regulatory partners like the U.S. Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC). As such, the FBI embedded Supervisory Special Agents and analysts within the SEC and CFTC to conduct real-time review of complaints and tips received by these agencies to determine if the information is relevant to an ongoing FBI investigation or should be referred for the opening of a new investigation. This greatly reduces the likelihood of relevant information slipping through the cracks. The placement of FBI personnel within these key regulatory agencies allows for earlier FBI involvement in parallel investigations and increases opportunities for the successful use of proactive and sophisticated techniques in complex investigations.

INVESTIGATING MULTINATIONAL COMPANIES

Question. The FBI is sometimes tasked with investigating very large, complex multinational companies, which could cost millions to investigate thoroughly. How does the FBI work with larger corporations in investigating criminal activity? How dependent is the FBI on information obtained through the internal investigations of companies? Does the FBI have adequate personnel to verify information provided by companies in their internal investigations? Could you please identify some examples of when the FBI has brought on experts from other agencies to assist in such investigations?

Answer. It is true that the nature of financial crime is becoming more complex than ever before. The complexity is driven by the nature of the offenses, the use of technology and more frequently, the international scope of investigations. Companies may serve as witnesses, victims, or as the targets of investigations. Regardless of the role, if the company is not deemed to be inherently criminal in nature, e.g., an established corporation with legitimate business interests versus a corporation created for the sole purpose of operating a Ponzi scheme, the company can serve as a tremendous source of information and a resource that can be leveraged to develop a more efficient investigative strategy. For example, cooperating companies, through their internal investigations, can review documents, identify witnesses, and provide an initial analysis of data. Although these efforts on the part of the company can aid an investigation, it would be inaccurate to describe the relationship as one where the FBI is dependent on the company and its internal investigation. The FBI has alternative methods to relying on the company's cooperation. For example, the FBI can collect records via a search warrant (given appropriate authority). Voluntary production of records can be mutually beneficial to both the Government and the company, but it also introduces the risks of completeness and accuracy of the data produced. Given that the company is likely not impartial, the investigative strategy must address these added risks. These risks can be addressed through a number of investigative methods, including interviews, independent verification from an external source, detailed descriptions of the internal investigation process with company counsel, and/or conducting our own analysis of the records.

FBI investigations into Complex Financial Crimes typically involve a number of FBI personnel, to include Special Agents, Forensic Accountants and Intelligence Analysts. The FBI also works closely with prosecuting offices and regulating agencies such as the Security Exchange Commision (SEC). The FBI regularly leverages experts and industry specialists from regulatory agencies conducting parallel investigations of Complex Financial Crimes. The use of these experts and industry specialists ranges from witness testimony during trial to serving as a resource during the investigation. For example, the FBI has utilized individuals from the Financial Industry Regulatory Authority-Criminal Prosecution Assistance Group (FINRA–CPAG) to analyze financial data, assess the risks associated with certain types of securities investments, review private placement agreements, and create summary data for trial. Economists and industry experts from the CFTC have identified, analyzed, and reported on brokerage records and provided technical assistance on investigations of commodity fraud. Industry specialists from the SEC have analyzed financial statements and served as Government witnesses during insider trading investigations. The FBI has also utilized the National Futures Association (NFA) for expert testimony on matters involving commodity fraud.

MORTGAGE FRAUD CASES

Question. In fiscal year 2013, the number of suspicious activity reports (SARs) related to mortgage fraud dropped 25 percent to just over 69,000, but could you pro-

vide a breakdown of how many SARs were investigated, bundled into a larger investigation, or were found to have insufficient information for investigation? Is there a backlog of cases the FBI plans to pursue from this surge of SARs following the financial crisis?

Answer. The FBI does not track, at the individual SAR level, whether SARs generate cases or are bundled into larger investigations. Each SAR filing does not equate to predication to initiate an investigation as an individual SAR may not provide enough information to open an investigation or multiple SARs may lead to one investigation. The FBI is unable to address every complaint of mortgage fraud, but attempts to work higher level cases which involve multiple victims, higher dollar losses or fraud activity, and/or target organized groups involved in the fraud. SARs are a valuable tool in identifying such networks but very often multiple SARs are associated with one group; therefore, these multiple SARs would be utilized to initiate one FBI investigation.

The FBI does not track the quality or sufficiency of SAR data other than to assess whether they can be utilized for lead value and therefore incorporated into new or existing investigations. The FBI does not currently have a backlog of cases from SARs associated with the financial crisis.

FOLLOW-UP ON DEFERRED AND NON-PROSECUTION

Question. How does the FBI conduct follow-up on non-prosecution and deferred prosecution agreements to ensure that companies are making the necessary reforms?

Answer. As elements of some deferred prosecution agreements (DPAs) and non-prosecution agreements (NPAs), companies are required to engage in remediation or compliance reforms. In such agreements, the Department of Justice includes a mechanism to ensure that companies may be taking the required actions. Generally speaking, this mechanism takes one of two forms: an independent compliance monitor who reports to the Department on a regular basis, or Department oversight, supported by mandatory self-reporting by the company on its efforts.

As an example of a corporate monitorship, in a December 9, 2013 DPA resolving Foreign Corrupt Practices Act (FCPA)-related charges against Bilfinger SE (“Bilfinger”), Bilfinger agreed to retain a corporate monitor for not less than 18 months. The monitor’s mandate under the DPA is to evaluate “the effectiveness of the internal accounting controls, record-keeping, and financial reporting policies and procedures of the company as they relate to the company’s current and ongoing compliance with the FCPA and other applicable anti-corruption laws[,]” including an assessment of the executive board’s and senior management’s commitment to, and effective implementation of, the corporate compliance program imposed as part of the DPA. Furthermore, under the DPA, the monitor is required to consult regularly with, and disclose any violations of law to, the Department. If the monitor concludes that the company has not instituted effective reforms or has engaged in further misconduct, then the monitorship may be extended or other action taken. Otherwise, the monitorship ends at the conclusion of the 18 month period and, for the remaining 18 months of the DPA, Bilfinger is required to self-report to the Department in a manner consistent with that described below.

As an example of oversight and self-reporting, in an April 9, 2014 DPA resolving Foreign Corrupt Practices Act (FCPA)-related charges against Hewlett-Packard Polska, SP. ZO.O. (“HP Poland”), HP Poland is required to report to the Department annually during the 3-year term of the DPA regarding its “remediation and implementation of the enhanced compliance measures” that it agreed to undertake as part of the DPA. The Department, in its sole discretion, determines whether the terms of the DPA have been met. Pursuant to a reporting schedule established in the DPA, HP Poland is required to “submit to the Department a written report setting forth a complete description of its remediation efforts to date, its proposals reasonably designed to improve the company’s internal controls, policies, and procedures for ensuring compliance with the FCPA and other applicable anti-corruption laws, and the proposed scope of the subsequent reviews[,]” which shall “further monitor and assess whether the company’s policies and procedures are reasonably designed to detect and prevent violations of the FCPA and other anti-corruption laws.” Moreover, the DPA provides that, “should the company discover any evidence or allegations of possible corrupt payments, false books and records, or the failure to implement or circumvention of internal accounting controls, including the existence of internal or external investigations into such conduct, the company shall promptly report such evidence or allegations to the Department.”

Department prosecutors review the monitor reports and corporate self-reports, meet with the monitor and/or corporate representatives as appropriate to follow up

on issues identified in the reports, and initiate further investigation where warranted. Under the terms of DPAs and NPAs, if the Department determines that a company has not made the required reforms, or has engaged in further misconduct, the Department has a range of options it may pursue, including but not limited to extending the terms of the DPA or NPA or declaring the company in breach of the DPA or NPA and instituting criminal prosecution against the company.

OIG REPORT

Question. Has the FBI taken steps to raise the prioritization of mortgage and mortgage-related securities fraud within its various field offices?

Answer. In its response to the OIG report, the Department noted that it has focused successfully on mortgage fraud violations. As the FBI data in the audit report itself reflects, the number of mortgage fraud convictions more than doubled from fiscal year 2009 to fiscal year 2010, i.e., from 555 to 1,087 convictions, and then increased further in fiscal year 2011 to 1,118 convictions. In addition, the Department concurred with all of the recommendations made by OIG including: ensure all agencies update online and other publicly available material related to the Distressed Homeowner Initiative; revisit results of Operation Stolen Dreams to determine if corrective action on publicly reported results is necessary; implement methodology for properly soliciting, collecting and reviewing information; revisit existing guidance on initiating mortgage fraud undercover operation; and develop a method to readily identify mortgage fraud criminal and civil enforcement efforts for reporting purposes.

With respect to prioritization, in 2011, mortgage fraud was ranked as a priority area under the Criminal Investigative Division's Complex Financial Crime category. Not every type of fraud was ranked as a priority threat during this time period, which demonstrates that the FBI considered mortgage fraud to be among the most prominent financial crimes we faced at the time.

We also recognize that the Inspector General contended that mortgage fraud was a low priority or not listed as a priority at various FBI Field Offices, including the Baltimore, Los Angeles, Miami, and New York offices. We note, however, that during the period covered by the audit, all threats were prioritized at the headquarters level, and that FBI field offices did not re-rank threats within their own geographical areas. As noted above, mortgage fraud was ranked as a priority threat, and the various field offices would have utilized that prioritization instead of coming up with their own rankings. Beginning in 2013, however, FBI field offices were required to rank their own threats based on domain assessments, ongoing intelligence collection and ultimately, with approval from FBI Headquarters. We can report that Baltimore, Los Angeles, Miami, and New York all rank mortgage fraud as a priority threat.

QUESTIONS SUBMITTED BY SENATOR RICHARD C. SHELBY

CYBER SECURITY EFFORTS WITH PRIVATE INDUSTRY

Question. Given the growing cyber security threat facing our Nation and the challenges inherent in facilitating private industry reporting of attacks what is the FBI doing to facilitate participation in the EGuardian program?

Answer. Uniquely tailored for the particular challenges of cyber, the "Guardian for Cyber" application expedites the triage and deconfliction of leads submitted from multiple sources, which are then immediately assigned and assessed by the FBI and other government agency (OGA) partners. The system now includes secure, cyber-specific incident submission portals that consolidate critical information provided by both law enforcement (eGuardian) and trusted industry stakeholders (iGuardian). This response provides information regarding engaging the private industry with iGuardian.

The FBI's trusted industry partners have access to iGuardian, a secure method to report cyber intrusions and submit malware for analysis and feedback through the InfraGard Network. InfraGard is a partnership among the FBI and the private sector, educational institutions, local, State, and Federal Government organizations that are dedicated to protecting our national critical infrastructure by sharing information regarding both cyber and physical threats and vulnerabilities. InfraGard has a current active membership base of approximately 25,000 members.

At the request of FBI's private industry partners, the FBI has presented iGuardian overviews to critical infrastructure associations, alliance councils, and conferences. The interest to join the iGuardian portal has been significant. From concept to development, the FBI has been working with these partners through a

collaborative process to build a system to fulfill their needs. Every step of the way we have sought and incorporated private industry input.

The FBI is executing an iGuardian pilot program with five cleared facilities and is scheduled to be launched through an enhanced portal on FBI.gov. Once launched, the FBI will initiate the process for industry to apply for access through FBI.gov. Additionally, the FBI is in the process of enhancing the portal to be utilized to report multiple hazards, to include Counterterrorism, Counterintelligence, Criminal, and Cyber.

Question. Is this system open to all industries for reporting of cyber attacks? If not, what industries are participating? Is there a schedule to assimilate all industries into the system?

Answer. The system is accessible to all industries through the FBI's InfraGard network. The enhanced iGuardian portal, to be used by general industry, in addition to InfraGard members, has been launched. Five large, cleared facilities have provided their assistance to the FBI in enhancing this portal and piloting its initiation. This will significantly expand the Federal Government's increased awareness of vulnerabilities in critical infrastructure networks, to better understand cyber-related threat vectors, and to facilitate a coordinated overall cyber incident response by the U.S. Government. The FBI anticipates the Defense Security Service (DSS) will support the iGuardian portal as a threat submission tool that could be used by all cleared facilities. This will satisfy numerous existing requirements described in the National Industrial Security Program Operating Manual (NISPOM), section 941, among others.

The FBI is working as quickly as possible to fill the need to assimilate all industry into the iGuardian system, but there is no timeline established.

Question. Are there currently any requirements for industry to report cyber attacks? If so, what are those requirements?

Answer. The FBI is not aware of any requirement for industry to report to the FBI.

Question. Do you have any way of knowing the percentage of attacks on each entity or industry that are actually reported?

Answer. Due to the lack of required reporting by industry, the total number of cyber attacks made against entities and industries is unknown. Therefore, the Cyber Division cannot estimate the percentage of cyber attacks that are not reported to the FBI. However, based on data collected thus far, currently there are more than 4,100 reported incidents in Guardian categorized by sector, e.g. commercial sector, information technology, cleared defense contractors, Internet service providers, public health, financial services, education, and communications.

CYBER SECURITY

Question. Cyber security has topped the Director of National Intelligence's list of global threats for the second consecutive year. However, the FBI's mission prioritization does not seem to reflect the significance of the cyber threat we are facing. What's more, the budget request flat lines this growing threat. What reassurance can you give us that your mission prioritization is evolving with the threats our country is facing? Does this budget adequately resource the needs of the Bureau in key areas such as cyber security?

Answer. Through the support of the Congress, the FBI received funding in fiscal year 2014 that ended the hiring freeze and allows FBI to start hiring again. The fiscal year 2014 hiring effort will include personnel who will be dedicated to cyber efforts. Additionally, the fiscal year 2014 appropriation included a program increase to support the Next Generation Cyber Initiative. These fiscal year 2014 resources are critical to enhancing the FBI's cyber capabilities in the face of the growing cyber threat. The fiscal year 2015 President's budget request includes funding to sustain the critical improvements and enhancements in cyber security provided in fiscal year 2014. Cyber Security remains an FBI priority in fiscal year 2015.

The FBI's Cyber Division has developed and is implementing a new strategy, the Cyber Threat Team model, in which named threats are explicitly prioritized using an objective model, specialized teams of dedicated Field and HQ personnel are built for the highest priority threats, and detailed and explicit mitigation strategies are developed and implemented against these high priority threats.

HAZARDOUS DEVICES SCHOOL

Question. Could you detail the training capacity of the Hazardous Devices School today? Specifically, the number of students that it can accommodate, the number of classes offered annually and the need that exists in terms of re-certifying bomb technicians?

Answer. The current maximum throughput for the Hazardous Devices School (HDS) using the current curriculum is 1,214 students. HDS intends to operate at capacity in fiscal year 2015. In fiscal year 2014, HDS is operating slightly below capacity due to cancellations in October 2013 during the lapse in appropriations, and will train 1,014 bomb technician students in the following courses:

—6 Bomb Technician Certification Courses (six weeks), instructing 24 students per class—(maximum capacity: 8 classes);
—28 Bomb Technician Recertification Courses (one week, required every 3 years for certified technicians), instructing 24 per class—(maximum capacity: 30 classes);
—1 Bomb Squad Commanders class for 30 students;
—6 Stabilization Level III classes, with 12 students per class;
—4 Advanced Electronic classes, with 12 students per class—(maximum capacity: 6 classes); and
—3 Electronic Countermeasure (ECM) classes, with 16 students per class—(maximum capacity: 8 classes).

Regarding the need for FBI's training at HDS, the FBI has approximately 1,300 students on the waiting list for its certification and/or recertification classes.

Question. Is there an unmet training need in the bomb tech community and if so, are there sufficient resources in the budget request to meet that need? If not, please detail the unmet need and what additional resources would be required to do so.

Answer. The Stabilization and Electronic Countermeasure (ECM) courses require the use of temporary duty FBI Special Agent Bomb Technician instructors, because the full-time instructor cadre at HDS is stretched to capacity to keep up with the certification and recertification course schedule. Also, HDS can only offer two operational classes at any given time because the school's equipment, vehicles, storage, and training facilities are used to capacity. At this time, there is an eleven-month waiting period for bomb technicians to attend the recertification course, a twelve-month backlog for the certification course, and a 6 to 7-month waiting list for the Advanced Electronics and ECM courses.

As the domestic Improvised Explosive Device (IED) environment evolves, the need for advanced instruction to address sophisticated explosive device designs and attack methods continue to grow. Based on intelligence gathered from around the globe and exploited by the Terrorist Explosive Device Analytical Center (TEDAC), the FBI has developed several advanced courses for bomb technicians with a focus on standardized tactics, techniques, and render safe procedures (RSPs). These advanced courses focus on real, complex threats, such as vehicle-borne, water-borne, and radio-controlled IEDs, suicide bombers, homemade or improvised explosives, weapons of mass destruction, and scenarios that require bomb technicians to operate side-by-side with tactical teams. Advancing FBI instruction at HDS is crucial to effectively meet the needs of the U.S. bomb technician community by teaching standardized operating procedures for bomb squads to defeat these threats. Central certification and curriculum development will also reduce training costs to both public safety bomb squads and the Federal Government. The FBI continues to evaluate resource needs and will work to expand the delivery of this advanced training to public safety bomb technicians within available resource levels.

QUESTIONS SUBMITTED BY SENATOR MARK KIRK

ONLINE SEX TRAFFICKING

Question. Approximately how many FBI agents are designated to sex-trafficking investigations?

Answer. The FBI has more than 400 agents designated to investigations involving the abduction or disappearance of children, online sexual exploitation of children and the commercial sexual exploitation of children, i.e. sex trafficking of children.

Question. How much funding is allocated to these sex-trafficking investigations?

Answer. In fiscal year 2014, the FBI will spend approximately $107 million on cases involving the abduction or disappearance of children, online sexual exploitation of children and the commercial sexual exploitation of children, i.e. sex trafficking of children. This amount includes both personnel and non-personnel resources.

Question. What Web sites has the FBI identified as the leading Web sites for Internet sex trafficking?

Answer. The FBI has identified more than 100 Web sites that cater to escort and sexual services advertisements. Many of these Web sites may focus on particular cities and/or regions, while others advertise escort and sexual services nationwide. In

addition to these Web sites, social networking Web sites and dating Web sites are also being utilized to facilitate the advertisement of prostitution. For an advertisement offering a commercial sexual service to constitute Federal criminal sex trafficking, the victim induced to commit such conduct must either be under the age of 18 or an adult subjected to force, fraud, and coercion. Since the FBI does not want to promote the Web sites, specific Web site information will not be provided.

Question. What is the FBI's determination of the percentage of ads posted on Backpage.com adult-services section is for prostitutes? What about other Web sites?

Answer. Federal investigative resources are focused on eradicating sex trafficking, which occurs when children engage in commercial sex acts and when adults are compelled to engage in commercial sex acts through the use of force, fraud, or coercion. In the course of investigating sex trafficking, the FBI does review advertisements on Web sites for adult services. Through the course of that review, the FBI has determined a significant number of the advertisements posted on the adult-services section of identified Web sites are specific to prostitution. In addition to advertisements, many of these sites also offer review boards wherein active members can review and rate "prostitutes," discuss popular areas and venues for prostitution, and post intelligence of law enforcement activity and methodology. The volume of prostitution advertisements on social networking and dating Web sites is more difficult to quantify as the advertisements are embedded within user profiles and are not always accessible to law enforcement due to privacy measures implemented by the user. As for the advertisements posted on other Web sites specifically for escorts, the FBI has determined a significant number these advertisements are also specific to prostitution.

SUBCOMMITTEE RECESS

Senator MIKULSKI. The committee recesses and we'll reconvene in the Visitors Center.

[Whereupon, at 10:48 a.m., Thursday, March 27, the subcommittee was recessed, to reconvene subject to the call of the Chair.]